



UNITED STATES PATENT AND TRADEMARK OFFICE

cen
UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/725,116	12/02/2003	Victor Gorelik		2789

7590
Dr. Victor Gorelik
Apt. C1
254 73 Street
Brooklyn, NY 11209

01/19/2007

EXAMINER

LOUIE, OSCAR A

ART UNIT

PAPER NUMBER

2112

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	01/19/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No. 10/725,116	Applicant(s) GORELIK, VICTOR	
	Examiner Oscar A. Louie	Art Unit 2112	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 02 December 2003.
- 2a) ☐ This action is FINAL. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-6 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-6 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 12/02/2003 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

This first non-final action is in response to the original filing of 12/02/2003. Claims 1-6 are pending and have been considered as follows.

Examiner's Notes

1. The Applicant appears to be attempting to invoke 35 U.S.C. 112 6th paragraph in Claims 5 & 6 by using "means-plus-function" language. However, the Examiner notes that the only "means" for performing these cited functions in the specification appears to be computer program modules. While the claims pass the first test of the three-prong test used to determine invocation of paragraph 6, since no other specific structural limitations are disclosed in the specification, the claims do not meet the other tests of the three-prong test. Therefore, 35 U.S.C. 112 6th paragraph has not been invoked when considering these claims below.

Claim Objections

2. Claims 5 & 6 are objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim. Applicant is required to cancel the claim(s), or amend the claim(s) to place the claim(s) in proper dependent form, or rewrite the claim(s) in independent form. The examiner notes that Claim 5 discloses, "the means for performing of twisted sampling and submitting data to the server according to claim 3," and, "the means for the client verification and/or identification according to claim 4," which fails as being of proper dependent form due to Claim 5 being a system where as Claims 3 and 4 are methods.

The examiner further notes that Claim 6 discloses, “the computer-readable program code for performing twisted sampling and submitting data to server according to claim 3,” and, “the computer-readable program code for client verification and/or identification according to claim 4,” which fails as being of proper dependent form due to Claim 6 being a computer program where as Claims 3 and 4 are methods. It is noted by the examiner that Claims 5 and 6 will be considered as independent claims where Claim 5 is a system and Claim 6 is a computer program with computer executable instructions stored on a computer readable storage medium for the rejections below.

Claim Rejections - 35 USC § 101

3. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

- Claim 6 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claim 6 of this application discloses a computer program comprising, “the computer-readable program code for performing twisted sampling and submitting data to server according to claim 3; and the computer-readable program code for client verification and or identification according to claim 4,” which is non-statutory subject matter in accordance to 35 U.S.C. 101.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. Claims 1-6 are rejected under 35 U.S.C. 102(b) as being anticipated by Buffam (US-6185316-B1).

Claim 1:

Buffam discloses a method for securely submitting biometric data from a client to a server comprising the steps of,

- Fig 8 (i.e. “performing sampling of a real biometric characteristic at the client”) [Fig 8].
- “Typically, an original image is represented by many discrete information points, similar to grid points on a map. True image points can be extracted from the information points on the basis of pragmatic considerations, such as data reduction. The set of true image points can be stored as a master template uniquely representative of the original image. False image points are generated and are selectively interposed among a chosen subset of the true image points, forming a transient template. The false image points also may be transformed to produce an encoding key.

It is most preferred that the encoding key itself is the result of imposing a hashing function on an ordered set of false image points that have been conditioned to be non-coincident with any true image point in the original image and to be plausible impostors

of the true image points. When properly interposed among the chosen true image points, the false image points are essentially indistinguishable from the true image points without reference to the master template, the original image, or complete knowledge of the false image points. These false image points thus form the basis for the secret encryption key. The encoding key can be used to encrypt a portion of plaintext into cipher text, and at least the cipher text portion can be added to the minutia points in the transient template” (i.e. “shuffling arrays of real biometric characteristics in the sequence known at client only to thereby generate twisted biometric data”) [column 12 lines 4-27].

- Fig 11 (i.e. “submitting the twisted biometric data from the client to the server”) [Fig 11 Box# 11].

Claim 2:

Buffam discloses a method for securely submitting biometric data from a client to a server as in Claim 1 above further comprising the steps of,

- “Typically, an original image is represented by many discrete information points, similar to grid points on a map. True image points can be extracted from the information points on the basis of pragmatic considerations, such as data reduction. The set of true image points can be stored as a master template uniquely representative of the original image. False image points are generated and are selectively interposed among a chosen subset of the true image points, forming a transient template. The false image points also may be transformed to produce an encoding key.

It is most preferred that the encoding key itself is the result of imposing a hashing function on an ordered set of false image points that have been conditioned to be non-

coincident with any true image point in the original image and to be plausible impostors of the true image points. When properly interposed among the chosen true image points, the false image points are essentially indistinguishable from the true image points without reference to the master template, the original image, or complete knowledge of the false image points. These false image points thus form the basis for the secret encryption key. The encoding key can be used to encrypt a portion of plaintext into cipher text, and at least the cipher text portion can be added to the minutia points in the transient template” (i.e. “shuffling sequence is calculated at client on the base of the value of a secret object created at the client and known to client only”) [column 12 lines 4-27].

Claim 3:

Buffam discloses a method for securely submitting biometric data from a client to a server as in Claim 2 above further comprising the steps of,

- “Typically, an original image is represented by many discrete information points, similar to grid points on a map. True image points can be extracted from the information points on the basis of pragmatic considerations, such as data reduction. The set of true image points can be stored as a master template uniquely representative of the original image. False image points are generated and are selectively interposed among a chosen subset of the true image points, forming a transient template. The false image points also may be transformed to produce an encoding key.

It is most preferred that the encoding key itself is the result of imposing a hashing function on an ordered set of false image points that have been conditioned to be non-coincident with any true image point in the original image and to be plausible impostors

of the true image points. When properly interposed among the chosen true image points, the false image points are essentially indistinguishable from the true image points without reference to the master template, the original image, or complete knowledge of the false image points. These false image points thus form the basis for the secret encryption key. The encoding key can be used to encrypt a portion of plaintext into cipher text, and at least the cipher text portion can be added to the minutia points in the transient template” (i.e. “step of multiplying the arrays of biometric characteristics by the sequences of numbers fixed for each type of array and known at the client only”) [column 12 lines 4-27].

Claim 4:

Buffam discloses a method for securely submitting biometric data from a client to a server as in Claim 3 above further comprising the steps of,

- Fig 11 (i.e. “step of submitting of twisted biometric data is followed by the step of comparing this data against the samples of twisted biometric data saved at the server previously, in such a way, that the result of the verification and or identification depends neither on the specific sequence in which biometric arrays were shuffled on the client, nor on the specific sequence of numbers used on the client to change the values of the arrays”) [Fig 11 Box# 11].

Claim 5:

Buffam discloses a system for secure use of biometric data comprising,

- “Typically, an original image is represented by many discrete information points, similar to grid points on a map. True image points can be extracted from the information points

on the basis of pragmatic considerations, such as data reduction. The set of true image points can be stored as a master template uniquely representative of the original image. False image points are generated and are selectively interposed among a chosen subset of the true image points, forming a transient template. The false image points also may be transformed to produce an encoding key.

It is most preferred that the encoding key itself is the result of imposing a hashing function on an ordered set of false image points that have been conditioned to be non-coincident with any true image point in the original image and to be plausible impostors of the true image points. When properly interposed among the chosen true image points, the false image points are essentially indistinguishable from the true image points without reference to the master template, the original image, or complete knowledge of the false image points. These false image points thus form the basis for the secret encryption key. The encoding key can be used to encrypt a portion of plaintext into cipher text, and at least the cipher text portion can be added to the minutia points in the transient template” (i.e. “the means for performing of twisted sampling and submitting data to the server according to claim 3”) [column 12 lines 4-27].

- “To self-authenticate, the claimant image is used to produce corresponding true image points that are extracted from the true image points of the original image held in the transient template. The residual image points include false image points. Candidate false image points (or minutiae) can be iteratively selected, and hashed to form a decryption key, with the decryption key operating on the cipher text to produce a result which is compared with the original, known plaintext. If the decryption result does not favorably

compare, the steps of candidate image point reselection, decryption key generation, cipher text decryption, and comparison with the known plaintext continues, until the pools of candidate false image points is exhausted, or a policy limitation is reached” (i.e. “the means for client verification and or identification according to claim 4”) [column 13 lines 6-19].

Claim 6:

Buffam discloses a computer program for secure use of biometric data comprising,

- “Typically, an original image is represented by many discrete information points, similar to grid points on a map. True image points can be extracted from the information points on the basis of pragmatic considerations, such as data reduction. The set of true image points can be stored as a master template uniquely representative of the original image. False image points are generated and are selectively interposed among a chosen subset of the true image points, forming a transient template. The false image points also may be transformed to produce an encoding key.

It is most preferred that the encoding key itself is the result of imposing a hashing function on an ordered set of false image points that have been conditioned to be non-coincident with any true image point in the original image and to be plausible impostors of the true image points. When properly interposed among the chosen true image points, the false image points are essentially indistinguishable from the true image points without reference to the master template, the original image, or complete knowledge of the false image points. These false image points thus form the basis for the secret encryption key. The encoding key can be used to encrypt a portion of plaintext into cipher text, and at

least the cipher text portion can be added to the minutia points in the transient template”
(i.e. “the computer-readable program code for performing twisted sampling and
submitting data to server according to claim 3”) [column 12 lines 4-27].

- “To self-authenticate, the claimant image is used to produce corresponding true image points that are extracted from the true image points of the original image held in the transient template. The residual image points include false image points. Candidate false image points (or minutiae) can be iteratively selected, and hashed to form a decryption key, with the decryption key operating on the cipher text to produce a result which is compared with the original, known plaintext. If the decryption result does not favorably compare, the steps of candidate image point reselection, decryption key generation, cipher text decryption, and comparison with the known plaintext continues, until the pools of candidate false image points is exhausted, or a policy limitation is reached” (i.e. “the computer-readable program code for client verification and or identification according to claim 4”) [column 13 lines 6-19].

Conclusion

6. The prior art made of record and not relied upon is considered pertinent to the applicant’s disclosure.

- a. Gennaro (US-6317834-B1)
- b. Thomlinson (US-6272631-B1)

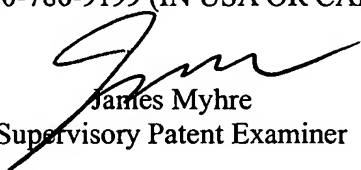
Art Unit: 2112

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Examiner Oscar Louie whose telephone number is 571-270-1684. The examiner can normally be reached Monday through Thursday from 7:30 AM to 4:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, James Myhre, can be reached at 571-270-1065. The fax phone number for Formal or Official faxes to Technology Center 2100 is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

OAL
01/11/2007


James Myhre
Supervisory Patent Examiner